UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

FILED 07 DEC 10 AM 11:52

CLERK, U.S. DISTRICT COURT SOUTHERN DISTRICT OF CALIFORNIA

BY: DEPUTY

'07 MJ 2862

UNITED STATES OF AMERICA, Plaintiff, v. TIMOTHY BYRON KALKA, Defendant	MAGISTRATE CASE NO.: COMPLAINT FOR VIOLATION OF Title 18, U.S.C. Section 1038 - FALSE INFORMATION AND HOAXES

The undersigned complainant, being duly sworn, states:

Count 1

On or about December 5, 2007, within the Southern District of California, defendant Timothy Byron Kalka, engaged in conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of perpetrating hoax devices, all in violation of Title 18, United States Code, Section 1038. And the complainant states that this complaint is based on the attached Affidavit incorporated herein by reference.

Heather Jackson, Special Agent
Federal Bureau of Investigation

SWORN TO ME AND SUBSCRIBED IN MY PRESENCE THIS 7th DAY OF DECEMBER, 2007.

BARBARA L. MAJOR
UNITED STATES MAGISTRATE JUDGE

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANT AND ARREST WARRANT

I, Heather A. Jackson , being first duly sworn, declares and states that:

INTRODUCTION

1. I am the Affiant herein, and I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to a FBI Counter-Terrorism Squad of the San Diego Division, having been employed by the FBI for approximately four (4) years. The following information was obtained by the Affiant and other law enforcement personnel.

2. For the past two years the Affiant has worked on a terrorism squad focusing primarily on domestic terrorism. The Affiant has received various training on domestic and international terrorism groups. The Affiant has also been the case agent in multiple FBI domestic terrorism investigations. I submit that the facts contained in the numbered paragraphs below demonstrate that there is probable cause to believe that fruits, instrumentalities, and evidence of violations of Title 18, U.S.C. 1038 (perpetration of hoaxes) will be found at the residence located at 4459 Manitou Way, San Diego, California (the residence of Timothy Byron Kalka, hereinafter referred to as "Target Location 1"). Target location 1 is further described in Attachment A, which I hereby incorporate by reference.

BASIS FOR THE FACTS CONTAINED IN THIS AFFIDAVIT

3. I make this affidavit, in part, based on personal knowledge derived from my participation in this investigation and, in part, based upon information from the following sources:

a. oral and written reports about this investigation and others that I have received from Detectives and Special Agents of the FBI, San Diego Police Department, Metro Arson Strike Team (MAST), and UCSD Police Department.

b. physical surveillance conducted by federal agents or local law enforcement agents, wherein observations have been reported to me either directly or indirectly;

c. witness interviews conducted by federal agents or local law enforcement agents, wherein interviews were conducted by me or reported to me.

4. Since this affidavit is being submitted for the limited purpose of securing court authorization for a search warrant to locate and seize fruits, instrumentalities, and evidence of perpetration of hoaxes, I have not set forth each and every fact learned during the course of the investigation. Nor have I summarized each and every factual circumstance deemed to be pertinent to the case. Rather, I have set forth only those facts that I believe are necessary to establish probable cause for the requested search warrant.

FACTS AND CIRCUMSTANCES ESTABLISHING PROBABLE CAUSE

A. INVESTIGATION OVERVIEW

5. On December 5, 2007, a hoax improvised explosive device (IED) was discovered at the Leichtag Biomedical Research Building (LBRB) located on the University of California at San Diego (UCSD) campus. Prior to the discovery of the device, four phone calls (including one voice message) were placed warning of "drastic action" against medical buildings located at UCSD. Additionally, a letter was received claiming that explosive devices had been placed in several buildings including the "Leichstad [sic] Research Building." After the device was determined to be a hoax device, the FBI released a copy of the voice message to the media. Numerous employees at the LBRB recognized the voice as belonging to Timothy Byron Kalka. Timothy Byron Kalka, is a former lab technician who, until recently, worked in LBRB. He was terminated from that position on November 30, 2007. On December 5, 2007, Kalka was observed in the LBRB at approximately 8:00 am and also seen walking away from the LBRB at approximately the same time the hoax improvised explosive device was discovered.

B. BACKGROUND ON TIMOTHY BYRON KALKA

6. Timothy Byron Kalka, date of birth September 25, 1957, was employed at UCSD as a lab technician working in the Leichtag Biomedical Research Building. His employment was terminated on November 30, 2007 because the University funding ran out for his research. Human Resources at UCSD provided Kalka's last known address as 4459 Manitou Way, San Diego, California.

7. According to the California Department of Motor Vehicles records, his current

driver license and vehicle registration address is 4459 Manitou Way, San Diego, California 92117. The 1990 Chevrolet Van bearing California license plate 6M89125 was registered to this address in September 2007.

8. Additional vehicles registered to Kalka include: (1) 1990 Honda RS Motorcycle , California license plate 15T4293; (2) 1983 Yamaha Motorcycle, California license plate 1Z1096; (3) 1986 Honda Motorcycle, California license plate 15E7627; (4) 1986 Suzuki Motorcycle, California license plate 12W1517; (5) 1987 Kawasaki Motorcycle, California license plate 13D4123.

9. On December 7, 2007, at approximately 3:30 p.m. FBI Special Agent Albert P. Scott observed the 1990 Chevrolet Van, California license plate 6M89125, parked approximately seventy-five (75) yards from 4459 Manitou Way, San Diego, California, on the adjacent street of Bannock Avenue. At approximately, 3:40 p.m. SA Scott observed an individual fitting the physical description of Kalka drive a motorcycle into the east garage at 4459 Manitou Way, San Diego, California. This individual exited the garage and entered into the front door of 4459 Manitou Way, San Diego, California.

10. As described more fully in Attachment A, Target Location 1 also includes a garage associated with 4459 Manitou Way, a yard associated with 4459 Manitou Way, and any outside structures.

C. PROBABLE CAUSE

11. On December 4, 2007, John Van Zante, Public Relations Manager for the Helen Woodward Animal Center received an anonymous voice message from a male caller stating the following: "John, you need to know that the American Animal Liberation Front is going to be doing a very drastic action against UCSD animal torture facilities in the medical schools and research centers. That's happening today. They have been told they need to take all the animals to a central animal location and a sanctuary would be there to help them relocate those animals. If not, there's going to be extreme consequences. So, I'm giving you a heads-up. Hopefully you all

will be there."

12. On December 5, 2007, between 8:00 a.m. and 9:00 a.m., the UCSD police department received a letter sent through inter-campus mail and signed with the letters "A.L.F". The first two lines of the typed letter read (in all capital letters), "WARNING! WE REPRESENT THE ANIMAL LIBERATION FRONT." The letter also threatened a "VERY DRASTIC ACTION ON UCSD MEDICAL SCHOOL AND RESEARCH FACILITIES." The letter claimed that the action had been planned for a long period of time and that they had the capability to execute the plan. The letter further threatened that a remote controlled explosive devices had been placed in six buildings at UCSD, to include the Leichtag Research Building. The letter continued on to say that if "THEY" did not see the evacuation of animals by 3:00 p.m, on 12/04/2007, "THEY WILL DETONATE REMOTELY ALL EXPLOSIVE DEVICES."

13. On December 5, 2007 at approximately 10:26 a.m., Shirley Reynolds, Lab Manager at the Leichtag Biomedical Research Building, called the UCSD police department to report the discovery of a suspicious device found in the Leichtag building. Initial analysis of the device by FBI Special Agent (and bomb technician), James G. Verdi was conducted at approximately 11:00 a.m. on December 5, 2007. SA Verdi observed what appeared to be an antenna attached to the device. Based on the stated threat of remote detonations, the presence of this antenna increased concern that this was a functional improvised explosive device.

14. As a result of the discovery of this device, the UCSD police department in conjunction with the San Diego Police Department evacuated several buildings. At approximately 3:30 p.m. the Metro Arson Strike Team (MAST) further examined and x-rayed the device and determined the device to be a hoax improvised explosive device.

15. The hoax explosive device is a 1.02 pound Coleman camping fuel cylinder (presumed empty) with four 12 gauge shotgun shells taped to the outside of the cylinder with yellow masking tape. Additionally, wires with audio plugs were also taped to the fuel cylinder along with what appears to be a television antenna and cable. The hoax improvised explosive device was place into FBI evidence on December 5, 2007. Additionally, the FBI took ash collecting sticky mats that may contain footprints into evidence. The FBI also collected the letter and envelope that was sent to the UCSD police department. The letter and mats have been sent to the FBI Laboratory for forensic analysis.

16. On December 6, 2007, the San Diego FBI released to the media a copy of the threat letter and voice message left for John Van Zante at the Helen Woodward Animal Center in hopes of eliciting investigative leads.

17. Jessica Porras is the vivarium supervisor of the Marth Lab in the Leichtag Vivarium located in the Leichtag Biomedical Research building. On December 7, 2007, Porras arrived at work at approximately 8:00 AM. Upon arriving at work, a co-worker by the name of Ryan Leaf pulled her aside and played a copy of the internet version of the voice mail message that was found on the KFMB 8 website and asked Porras if she recognized the voice. Porras listened to the recording and without any prior discussion regarding who the voice might belong to, she identified the voice to that of her co-worker Timothy Kalka. Porras also recalls seeing Kalka on December 5, 2007, at his work locker at approximately 8:00 A.M. Furthermore, at approximately 10:30 AM as the fire alarms were going off to evacuate the Leichtag building, Porras recalls seeing Kalka walking away from the Leichtag Biomedical Research Building (LBRB) smiling and laughing. Porras describes Kalka as a "very serious and grouchy person" and stated that this behavior was out of character for him. Porras did not find out that Kalka had been terminated from his employment at UCSD until December 7, 2007. Investigators showed Porras a driver license photograph of Timothy Byron Kalka and confirmed that he is the person she identified as her co-worker Timothy Kalka.

18. Freddie Vanta is a senior animal technician at UCSD. Vanta has been working at the LBRB for past three years. On December 6, 2007, Vanta was watching the local Channel 8 news broadcast on television when he heard the voice mail message. Immediately after hearing the voice mail message on television, Vanta turned to his wife and remarked, "I know that voice, I work with him." On December 7, 2007, Vanta discussed with his co-worker Stuart Kerns the voice mail tape released by the media and both agreed that the voice sounded like a co-worker named Tim Kalka.

19. On December 7, 2007, investigators played for Vanta a voice mail recording identical to the one that was released to the media. Vanta told investigators, "it sounds exactly like him (Tim Kalka)." Vanta stated that he was 100% sure the voice on the recording was Kalka.

Vanta also recalled seeing Kalka at his locker at approximately 6:00 AM on December 6, 2007, the day after the device was found. Vanta did not know Kalka's employment had been terminated. Vanta describes Kalka as always being "grumpy" and complaining about management.

20. Stuart Kerns works in animal care at UCSD in the Leichtag Building. Kerns has been working at the LBRB for two years. On December 7, 2007, Kerns was driving to work at approximately 5:45 AM with a co-worker, Ryan Leaf. As they were driving into work they heard the voice mail recording on KOGO radio. Kerns initially thought that the voice sounded familiar, but after arriving at work, discussing it with Vanta, listening to the recording again, Kerns agreed that the voice sounded like the voice of Tim Kalka. Kerns also recalls that last week in the basement of LBRB he noticed that Kalka was killing all of his laboratory mice, as many as one hundred mice total. Kerns felt that was very unusual because Kalka has been reluctant to kill his mice when required in the past. Kerns also mentioned Kalka did not like working for Jamey Marth, who is the head of Kalka's laboratory division.

21. Christine Mata is the human resources director for the Marth Lab located in the LBRB. Mata has had several interactions with Kalka over the past couple of months to discuss his pending termination. Also over this time period, she has engaged in several telephone conversations with Kalka. On December 7, 2007, investigators played the voice mail recording to Mata and she is confident that the voice is that of Tim Kalka.

DIGITAL EVIDENCE

22. Based upon information related to me on December 7, 2007, by Craig Porter of the San Diego Digital Forensics Group (SDDFG), I know that digital evidence can be stored on a variety of systems and magnetic, optical and mechanical storage devices including, but not limited to, hard disk drives, floppy disks, CD-ROMs, DVD-ROMs, magnetic tapes, magneto optical cartridges, personal digital assistants, pagers and memory chips.

23. Craig Porter has informed me that Computer Forensic Agents (CFA) of the San Diego Digital Forensics Group has instructed me on the proper manner in which to safely transport any seized digital media to a secure Evidence Storage Facility.

24. Any computers or computer systems, as defined in Attachment "B", found at 4459 Manitou Way, San Diego, California 92117 will be seized, transported from the scene, imaged at the SDDFG, and examined. This procedure is justified for two reasons. First, as set forth above, there is sufficient probable cause to show the Court that the computers and computer systems contain contraband, constitute evidence of the commission of a criminal offense, and/or were used as the means of committing a criminal offense.

25. Second, searching computers and computer systems is a highly technical process that requires specific expertise, equipment and software. There are a multitude of different types of computers manufactured today, many of which use proprietary hardware and software during the creation of any user data. It is impracticable for the law enforcement community to have all the proper adapters, cables, cords and other hardware devices necessary to consistently link law enforcement forensic equipment with all known and unknown computer systems on an immediate basis while searching "on-site." Much of this specialized equipment is available, but may need to be acquired in order to conduct a proper forensic examination.

26. There are literally thousands of different software programs that can be commercially purchased and installed on a user's computer system. As computer security has become an ever-increasing priority to many consumers, much of today's commercially available software is developed for, or provides, data security and encryption which makes it difficult to afford an accurate representation of any digital evidence confronted with on-site. Moreover, it is not feasible for a Computer Forensic Examiner to be familiar with every software program, past or present, now commercially available. It may be necessary for a CFA to train with a particular type of software in order to fully understand the capabilities of that software.

27. In order to safeguard the integrity of a computer forensic examination, it is imperative that the CFA first make a complete image of the original digital evidence before conducting a forensic examination. The CFA must ensure that any images made are forensically sound and that these forensic images can be fully restored, if necessary. There are numerous pitfalls that can seriously hamper the integrity of the imaging process while on-site. For example, to make a forensically sound

image of targeted original digital evidence, the CFA must ensure that there is an adequate uninterruptible power supply. Digital evidence is extremely fragile and susceptible to power interruptions or power surges. It is not always practical for a CFA to bring backup power supplies into the field.

28. Additionally, it may be necessary for the CFA to have unrestricted access to the original digital evidence during the course and scope of the forensic examination. There are numerous operating systems now being used by consumers. Some of these operating systems include, but are not limited to, DOS, Windows 3x, Windows 9x, Windows NT, Windows 2000, Macintosh, Linux, Unix, Novell and PICK. These operating systems use different file structures, different partition formatting and different file commands. Moreover, many of these operating systems are "hardware" specific. This means that a restored image of original digital evidence may not be "bootable" or "viewable" without the actual original hardware. This would prevent the CFA from viewing the restored digital image in a manner consistent with the structure of the original digital evidence. This problem is especially acute when dealing with operating systems like Linux, Unix, MAC and Novell.

29. These problems are accentuated by the fact that it is possible for a user to have two or more different operating systems on the same piece of original digital evidence. This severely hampers the CFA's ability to image this type of original digital evidence on-site due to certain software limitations. This type of problem generally requires that the imaging process take place in a controlled environment, such as the SDDFG. Once this procedure is completed, a CFA can then safely conduct most types of requested examination using this newly created "image" file without fear of damaging, destroying, adding or altering any files or operating system components of the original digital evidence.

30. It is also very difficult in today's computer environment to "search" for specific data while on-site. To conduct any type of digital "search" without using a forensically created image predisposes multiple forensic problems. It may literally take hours, if not days, to appropriately search a medium to large size hard drive for any desired data. For example, a search for the word "kill" during a homicide investigation could find thousands of positive hits, due to the fact that while a subject may have in fact wanted to kill the victim. The term "kill", however, is also a valid computer

command related to the ending of an otherwise innocuous computer process.

31. Computers can be difficult to examine even if no serious effort is used to conceal or protect its digital contents. A complete forensic search is not limited to examining files normally displayed by the operating system. It also includes the expansion of compressed data and the recovery of deleted file data. It involves the areas on a computer hard drive that the computer system recognizes as being "in use" and those areas that the computer that the computer system deems "available for use." This search may involve an examination of "slack" space, which is the information at the end of a sector or cluster beyond the end of the "current" usage. Finally, the complete examination would address "orphaned" data, portions of files left behind by earlier operating system activity. All of these areas require operating specific tools and techniques to access the data.

32. It is also very easy for a computer user to conceal data or other types of digital evidence through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension "jpg" are digital image files. A moderately sophisticated computer user, however, can easily change the .jpg file extension to "txt" or "dll" in order to conceal or mislead law enforcement into thinking the digital image is actually a text or system file. While it is may be possible for a CFA to notice this during a properly controlled forensic examination, it is difficult for that same CFA to detect this concealment during an on-site examination. For example, the Windows 9x Operating System, installed right out of the box, would itself contain over 20,000 different system files. A devious user could then alter any improper files so as to make them appear to be legitimate files.

33. The problems noted above are compounded by the fact that the volume of data stored on a typical computer system is so large that it would be unrealistic to search for specific data while conducting an on-site examination. For example, a single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now capable of storing more than 60 gigabytes of data and are commonplace in new desktop computers.

34. Additional problems are created by the growing use of destructive programs or "booby traps." These programs can destroy or alter data if certain forensic procedures are not scrupulously followed. Since digital evidence is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as the SDDFG, is essential to conducting a complete and accurate examination of any digital evidence. This problem mandates that all examinations need to take place using only a forensic image of the original digital evidence.

35. Finally, there is also a growing use of military-grade encryption by consumer and commercial computer users. These encryption programs, which are low or no cost, are widely available and allow users to encrypt specific data with just a few keystrokes. These encryption problems are accentuated by other newer technologies, like steganography, which allows a user to conceal information within other files. It is difficult to detect the use of this technology without a proper forensic examination and the ability to look at the entire image of the subject digital evidence.

36. For the reasons set forth above, I respectfully request that I be allowed to seize all computers and computer systems, as defined in Attachment "B," and transport them to the SDDFG for a proper forensic examination including imaging and searching.

Heather A. Jackson, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and **SWORN** to before me,
this 7th day of December, 2007

UNITED STATES MAGISTRATE JUDGE